Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-28 (Cancelled).

Claim 29 (Currently amended): A method for reducing vulnerability of a Virtual Private Network (VPN) protected network to attack by an end system, comprising the steps of:

permitting access by an end system to a VPN protected network on at least one VPN connection in response to authenticating a user of the end system to the VPN protected network; and while permitting the access:

continuously monitoring on the end system for attempted writes to the end system and preventing detected attempted writes to permanent memory on the end system;

continuously monitoring on the end system for traffic on the end system and filtering detected traffic ~~inbound to~~ received on the end system that is not on the VPN connection; and

continuously monitoring on the end system for termination of the VPN connection and purging temporary memory on the end system in response to detected termination of the VPN connection whereby malicious code written to temporary memory while permitting the access is eradicated from the end system.

Claim 30 (Previously presented). The method of claim 29, wherein the step of continuously monitoring for attempted writes to the end system further comprises redirecting to temporary memory detected attempted writes to permanent memory.

Claim 31 (Previously presented): The method of claim 29, wherein the step of continuously monitoring for traffic on the end system further comprises filtering detected traffic outbound from the end system that is not on the VPN connection.

Claim 32 (Previously presented): The method of claim 29, further comprising, before permitting the access, the step of denying network access except for performing user authentication.

Claim 33 (Previously presented): The method of claim 29, wherein the monitoring steps are performed by the end system.

Claim 34 (Previously presented): The method of claim 33, wherein the monitoring steps are performed by software having instructions executable by a processor.

Claim 35 (Previously presented): The method of claim 34, wherein the software is embedded in permanent memory.

Claim 36 (Previously presented): The method of claim 35, wherein the software is adapted to inhibit modification of the software by the user.

Claim 37 (Previously presented): The method of claim 29, wherein the step of monitoring for termination further comprises logging-off the user in response to detected termination of the VPN connection.

Claim 38 (Previously presented): The method of claim 29, wherein the step of monitoring for termination further comprises rebooting the end system in response to detected termination of the VPN connection.

Claim 39 (Previously presented): The method of claim 29, wherein the step of monitoring for termination further comprises shutting down the end system in response to detected termination of the VPN connection.

Claim 40 (Previously presented): The method of claim 29, wherein permanent memory comprises a flash memory.

Claim 41 (Previously presented): The method of claim 29, wherein temporary memory comprises a random access memory (RAM) disk.

Claim 42 (Currently amended): A VPN capable end system, comprising:

at least one permanent memory;

at least one temporary memory;

at least one processor coupled to the permanent memory and the temporary memory; and

software stored on the permanent memory, the software having instructions executable by the processor while the end system is permitted access to a VPN protected network on at least one VPN connection to continuously monitor for attempted writes to the end system and prevent detected attempted writes to the permanent memory, to continuously monitor for traffic on the end system and filter detected traffic ~~inbound to~~ received on the end system that is not on the VPN connection, and to continuously monitor for termination of the VPN connection and purge the temporary memory in response to detected termination of the VPN connection whereby malicious code written to the temporary memory while permitting the access is eradicated from the end system.

Claim 43 (Previously presented): The end system of claim 42, wherein the software further has instructions executable by the processor while the end system is permitted

the access to redirect to the temporary memory detected attempted writes to the permanent memory.

Claim 44 (Previously presented): The end system of claim 42, wherein the software further has instructions executable by the processor while the end system is permitted the access to filter detected traffic outbound from the end system that is not on the VPN connection.

Claim 45 (Previously presented): The end system of claim 42, wherein the software further has instructions executable by the processor while the end system is not permitted the access to deny network access to the end system except for performing user authentication.

Claim 46 (Previously presented): The end system of claim 42, wherein the software is embedded in the permanent memory.

Claim 47 (Previously presented): The end system of claim 42, wherein the software is adapted to inhibit modification of the software by a user of the end system.

Claim 48 (Previously presented): The end system of claim 42, wherein the software further has instructions executable by the processor while the end system is not permitted the access to facilitate authentication of a user of the end system to the VPN protected network.

Claim 49-54 (Cancelled).

Claim 55 (Currently amended): A VPN capable end system, comprising:

A plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory;

at least one processor coupled to the memories; and

software stored in the permanent memory, the software having instructions executable by the processor while the end system is permitted access to a VPN protected network on at least one VPN connection to continuously monitor for attempted writes to the end system and prevent detected attempted writes to the permanent memory, to continuously monitor for traffic on the end system and filter detected traffic ~~inbound to~~ received on the end system that is not on the VPN connection, and to continuously monitor for termination of the VPN connection and purge the temporary memory in response to detected termination of the VPN connection whereby malicious code written to the temporary memory while permitting the access is eradicated from the end system.

Claim 56 (Previously presented): The end system of claim 55, wherein the software further has instructions executable by the processor while the end system is permitted the access to redirect to the temporary memory detected attempted writes to the permanent memory.